

fraud alert

october/november 2004

**Phishers “net”
unsuspecting
consumers**

**Money launderers
threaten to sully
insurance industry**

Stop the till from running dry

**Fraud a big problem for small
businesses**

**FBI, CPAs become partners
in crime prevention**



McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

105 W. Madison Street, Suite 406
Chicago, Illinois 60602

Phishers “net” unsuspecting consumers

Internet fraud growing dramatically despite prevention efforts

“Phishing” — sending phony or “spoofed” e-mails that trick people into providing personal and financial information — is the fastest-growing Internet scam in the world. Between September 2003 and January 2004, the number of phishing e-mails soared from about 280 to more than 330,000, according to MessageLabs, an e-mail security company that monitors corporate e-mail traffic.

Research firm Gartner estimates that, as of May 2004, 57 million U.S. consumers had or suspected they had received phishing e-mails. More disturbing, phishermen have caught about 1.8 million unsuspecting souls in their nets.

Fast development

This insidious form of Internet fraud started relatively benignly a decade ago when America Online still charged users by the hour. Cash-strapped teenagers looking to stay online longer posed as AOL representatives in e-mails and went fishing (or phishing) for account identification and passwords that would allow them to surf the Web at someone else's expense.

When AOL switched to a flat monthly rate, phishers started looking for a bigger catch — credit card information.



The problem has become so pervasive that some 450 technology companies, financial institutions and law enforcement agencies banded together to form the Anti-Phishing Working Group (APWG) in November 2003. Internet provider EarthLink has launched its own major effort to track down perpetrators.

Unfortunately, these organizations haven't had notable success. Although investigators have traced a few individual phishers, organized professional crime gangs located in Eastern Europe and Asia are behind more sophisticated efforts and have proven almost impossible to apprehend.

Losses difficult to tally

Officials say it is impossible to calculate the amount phishers have stolen from unwary consumers — in part because fraudsters may wait up to six months to use the information they obtain.

Many times, losses are absorbed by banks and credit card companies, at a cost financial firms claim is less than that associated with other fraud, such as stolen charge cards. Still, according to one estimate, phishing cost U.S. banks and credit card companies approximately \$1.2 billion last year.

One large U.S. bank fielded up to 90,000 calls per hour after a phishing attack paralyzed the bank for five hours. Internet auction colossus eBay estimates it costs \$100,000 to respond to the roughly 20,000 phone calls it gets after every phishing attack directed at that company.

Though phishers fraudulently use the names of many legitimate companies, some names get abused more than others. About 30% of phishing e-mails involve eBay. Online payment service PayPal is cited almost as often — at 29% — while Citibank's name has been used in about 14% of cases.

How they do it

Typically, perpetrators send spam e-mails purporting to be from an actual business, often warning that an account will be closed or prosecution will

result if the recipient does not update information at that company's Web site.

Recipients may be provided with a link to a bogus, but real-looking, Web site where they are asked to enter personal information. Or the link might be to a legitimate Web site, but clicking on it triggers a key-logger program that captures log-in details. Either way, thieves get the information they need for identity theft or other fraudulent activities.

Phishing prevention

Although technology is being developed to thwart phishers, and consumer awareness is rising, experts acknowledge that it is unlikely they will be able to eliminate successful phishing expeditions altogether. (Even the best-informed consumer is unlikely to know that yahoo.billing.com is fake, but billing.yahoo.com is real, for example.)


To be safe, the APWG suggests consumers be suspicious of any urgent request for personal financial information online and avoid using links in such

The ones that didn't get away

While phishing scams are becoming more sophisticated and difficult to detect, authorities have succeeded in catching some phishers:

- A 55-year-old woman from Akron, Ohio, used mass e-mails purporting to be from the "AOL Billing Center" to obtain credit card information from America Online customers. She pleaded guilty to conspiracy and, in January 2004, was sentenced to 46 months in prison.
- A 20-year old Houston man used the names of AOL and PayPal to obtain more than 470 credit card numbers and at least \$75,000. In May 2004, he was sentenced to four years in prison.
- A Mankato, Minn., college student pleaded guilty to wire fraud after he used a key-logger program to obtain PayPal user names and passwords from at least 150 people. He paid a \$35,000 fine and received 18 months in prison.
- A man was sentenced to 30 months in a Romanian prison for stealing nearly \$500,000 from unsuccessful eBay bidders. The scam? He promised bidders similar merchandise at lower prices if they provided bank account numbers and passwords and wired money to his fake escrow site.

e-mails to access a Web page. They should also regularly monitor their financial statements for any unauthorized charges or withdrawals.

Finally, people need to report phishing or spoofed e-mails to the company whose name is being abused, the Federal Trade Commission (spam@uce.gov) and the APWG (reportphishing@antiphishing.org). 

Money launderers threaten to sully insurance industry

The insurance industry generates about \$2.5 trillion in premiums worldwide every year. That money is presumed to be clean — which is why the insurance industry is becoming more attractive to crooks seeking to launder ill-gotten gains.

Although officials say reported instances of money laundering in the insurance industry remain low, they disagree over whether that is due to lack of activity or lack of detection. But one thing is clear: The industry is too large and, in many ways, too vulnerable for launderers to overlook it forever.

Industry vulnerability

Insurance companies are particularly vulnerable to money laundering because their business is typically conducted by agents who aren't affiliated with the company that writes the policies. Agents and brokers simply may not understand when due diligence is required to unearth suspicious transactions.

In worst-case scenarios, agents willingly participate in criminal schemes for financial gain.

In addition, banks routinely accept payments — even international payments — that originate from insurance companies without raising an eyebrow. Finally, insurance companies' business is diverse, giving would-be fraud perpetrators a wider range of operation.

Three stages

Typically, there are three stages to laundering money:

- Placement, in which illegitimate money is paid into legitimate financial accounts,
- Layering, in which the money is disguised by being moved in numerous transactions through various products and institutions, and
- Integration, in which now-clean money is put back into circulation to fund other activities.



launderers establish a stream of “innocent” wire transfers or checks — all for the relatively low cost of penalties for early withdrawal.

In still other instances, the launderers name third-party beneficiaries on policies, overpay policy premiums and then request that reimbursements be made to those third parties.

Insurance companies are particularly vulnerable to money laundering because their business is typically conducted by agents who aren't affiliated with the company that writes the policies.

Know your customer

To protect against these and other, increasingly sophisticated forms of money laundering, insurers must, first and foremost, implement and insist on “know your customer” procedures. This means not only obtaining identification for all new accounts and monitoring those accounts for suspicious activity, but also revisiting the transaction records of existing customers periodically.

Criminals may target insurance companies in one of several ways. Launderers may use “dirty” money to buy insurance and then submit claims against that insurance to retrieve the funds.

In one case, for example, a money launderer paid large premiums to insure a phantom boat, then suborned intermediaries to assure payment of regularly submitted claims. To avoid detection, the launderer kept the claims lower than the premiums, thus assuring the insurance company a profit while maintaining a steady supply of seemingly untainted money.

In other cases, thieves take advantage of insurance products structured to serve as investments, such as variable annuities and life insurance policies. By overfunding and moving money in and out of policies, the

Warning signs include customers who frequently change beneficiaries, use policies as bearer assets or as collateral for wider schemes, or opt to cash in investment-type policies early, even when there is no financial advantage to doing so. Finally, firms should check whether customers are included on any watch lists maintained by U.S. and other law enforcement authorities.

Now more than ever

In the aftermath of 9/11, regulators worldwide have heightened their scrutiny of money launderers. The USA Patriot Act and anti-money-laundering legislation worldwide make it more important than ever that insurance companies know their customers' identities — including the source of their money. Having this knowledge is the best defense against money launderers attacking the insurance industry as a whole. ¶

Stop the till from running dry

Spotting and preventing cash register theft

Because many retail businesses implement careful controls over the use of their cash registers, register-disbursement schemes are among the least costly types of cash frauds. The absence of such controls, however, still leads to significant losses for many businesses.

One Texas department store learned this the hard way when internal auditors and outside fraud examiners uncovered an extremely costly employee theft scheme. A trusted store manager made daily register withdrawals — disguised as cash refunds — in amounts ranging from \$200 to \$700. Over a period of three years, he managed to steal a whopping \$800,000 — forcing the store to close because of unprofitability.

Spotting register schemes

The Texas store isn't alone in falling victim to this scheme. Issuing fictitious refunds or falsely voiding sales are common ways for employees to steal money. Both methods involve paying out cash without a corresponding return of inventory and usually result in abnormally high inventory shrinkage levels.

High shrinkage is just one indication of cash register disbursement fraud. Other red flags include:

- Disparities between gross and net sales,
- Decreasing net sales (increasing sales returns and allowances),
- Decreasing cash sales relative to credit card sales,
- Forged or missing void or refund documents,
- Altered cash-register tapes,
- Increasing void or refund transactions by individual employees, and
- Multiple refunds or voids just under the review limit.

Any of these warning signs may warrant investigation by internal auditors and outside fraud experts who can determine whether discrepancies have innocent explanations or indicate a more serious problem.

Prevention is the best cure

Businesses can head off employee theft by taking preventive measures. These include having written ethics policies and providing all employees with antifraud training. In many cases of register theft, several employees are aware of the problem, so it is essential to provide a confidential hot line or other means for employees to report unethical behavior without fear of reprisal.

A company's fraud detection and deterrence program should also include training internal auditors to regularly perform horizontal analysis of income statements. Horizontal analysis — which compares financial statement line items from one period to the next — can identify suspicious trends, such as an increase in cash refunds.



Get professional help

Taking these simple steps may save an organization a significant amount of money. But signs of extensive cash register theft probably indicate the need to call in a fraud examiner. These experts can both nip theft in the bud and, when necessary, assemble evidence for criminal prosecutions and civil lawsuits. ¶

Fraud a big problem for small businesses

Fraud is often considered a hidden cost of doing business. But for small businesses, it can easily get out of control and become a disabling problem.

According to the Association of Certified Fraud Examiners (ACFE), small businesses are the most vulnerable to occupational fraud and abuse. In its *2004 Report to the Nation on Occupational Fraud and Abuse*, ACFE reports that the smallest companies (100 employees or less) suffered higher median losses — \$98,000 per year — than did larger companies (10,000 employees or more). Cumulatively, U.S. small businesses lose billions of dollars through fraud every year.

Internal fraud

The first step in preventing fraud is understanding what it is. Fraud takes one of two general forms — internal or external.

Internal fraud can include asset misappropriation and corruption. With asset misappropriation, employees steal cash or noncash goods using a variety of techniques. One such technique is to trick the company into making fraudulent disbursements of cash by submitting bogus invoices or submitting timecards claiming hours not worked.

Corruption schemes, on the other hand, typically involve a dishonest employee who conspires with someone outside of the company. For example, purchasing agents and buyers are constantly barraged with offers of gifts and other enticements by vendors attempting to lure them to buy their products. Sometimes, these situations turn into outright graft and the victim company pays a bribe in the form of higher prices or substandard goods.

Preventing these forms of internal fraud can be relatively simple. You should always perform extensive background checks when hiring — particularly on employees who will handle money and inventory.

Strong internal controls are also essential. These include limiting the number of people authorized to sign checks and setting dollar limits on check amounts. And while you don't want to turn your business into a police state, security cameras in cash



register areas and storage rooms are good fraud deterrents.

External fraud

Business owners also have to worry about external fraud. The most common forms — check and credit card fraud — have grown remarkably in the past few decades, thanks to cheap and easily available desktop publishing equipment and a dramatic rise in identity theft.

You can protect yourself from these forms of external fraud by knowing your customer, and, barring that, carefully training employees to recognize signs of check and credit card fraud.

For checks, these include:

- Poor print quality and paper,
- Signatures that extend past the signature line, and
- Checks written on new accounts — usually those less than six months old.

Some signs of credit card fraud are:

- Cards that appear to have been flattened and restamped with different numbers,

- Alterations on the signature panel,
- Misspellings of company names or dates, and
- Pasted pieces of aluminum foil attempting to represent holograms.

Employees should also be suspicious of customers who make hurried or random purchases with little regard to quantity or value, make large purchases just under the approved card limit or sign their names on sales receipts slowly or awkwardly.

Finally, you should be aware of bust-outs — when fraudulent business customers buy large amounts of

merchandise and run up debts they have no intention of paying. The best protection against bust-outs? Don't extend credit to new or unverified businesses.

Limiting fraud's impact

You can't expect to root out fraud entirely. But recognizing its many forms and taking preventive measures can limit its impact. One of your primary forms of defense is a CPA, who can advise you about fraud prevention techniques. CPAs can also perform regular reviews to discover fraud schemes before they have a devastating effect on your business's profitability. 🔑



Fraud to watch for: FBI, CPAs become partners in crime prevention

The FBI is currently investigating more than 2,000 cases of securities and corporate fraud in the United States. But a new joint initiative by the FBI and the American Institute of Certified Public Accountants (AICPA) to share fraud-detection strategies, auditing techniques and other mutually advantageous information could help put a dent in that number.

Both organizations agree: Cooperation among accountants, law enforcement and businesses is essential if white-collar crime is to be detected and deterred.

Rising crime rates

White-collar crime is not new, but it has exploded in recent years. The Enron, WorldCom and Tyco scandals are just a few examples of the fraudulent activities that have grown to encompass millions of dollars and thousands of victims.

The Sarbanes-Oxley Act — which grew out of such scandals — and a new SEC regulation that requires outside auditors to test the strength of companies' internal fraud-detection procedures are just two of the tools that have given

authorities more muscle in recent years. But white-collar criminals are imaginative and fully capable of coming up with new schemes — keeping law enforcers on their toes.

CPAs are first defense

CPAs are the first line of defense in thwarting basic accounting fraud. They now are passing their objective professional skepticism along to the FBI for use in broader arenas. They also are teaching FBI agents to recognize and understand the significance of some recurring fraud themes, particularly in revenue recognition.

On its part, the FBI is sharing the latest fraud detection techniques, as well as calling on CPAs as third-party witnesses and eyewitnesses. The FBI notes that corporate fraud is not confined to Wall Street or Silicon Valley. Nor is it limited to a specific industry. Instead, fraudulent activities are being detected in businesses of every size and in every marketplace.

By sharing ideas and information, as well as manpower, the AICPA and the FBI will be better positioned to unearth new approaches to fraud before they reach catastrophic proportions.

McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

Specialists in Fraud Examination and Litigation Services

If a business hasn't yet been a victim of fraud, it's been fortunate. According to the Association of Certified Fraud Examiners, fraud costs businesses in the United States billions of dollars every year. Small businesses are especially vulnerable because they often do not have controls in place to reduce the likelihood of fraud.

This is where McGovern & Greene LLP can help. Our firm specializes in helping corporations, attorneys, lenders, law enforcement and governmental agencies analyze financial records and contracts, identify and prevent fraud, recover and analyze evidence, and provide expert testimony in all of these matters. Our highly-experienced team of professionals includes certified fraud examiners and certified public accountants that are experts in the fields of fraud examination, forensic accounting, computer forensics, damage calculations, business valuations and audit services.

Our professionals can assist you in a wide range of matters, including:

- Fraud Examination
- Financial Investigations
- Forensic Accounting
- Asset Recovery
- Internal Audit Services
- Computer Forensics
- Training & Seminars
- Healthcare Audit
- Business Valuation
- Litigation Services
- Government Contracts
- Economic Damages
- Intellectual Property
- Contract Claims
- Construction Audits
- Electronic Discovery
- Profit Recovery
- Due Diligence

We welcome the opportunity to discuss your needs and answer any questions you might have about our fraud examination and litigation services.

Please contact us at 312.419.1961 or visit us at www.mcgovernngreene.com and let us know how we can be of assistance.

McGovern & Greene LLP
105 W. Madison Street, Suite 406
Chicago, Illinois 60602

